Information Booklet

Using Western Resources on a COVID-19 Laptop Program Pre-Configured Computer

ITDS
March 2020

Contents

COVID-19: Information Technology and Digital Services Laptop Program and Working Remotely

This document outlines several technology programs and services to support the University community during the COVID-19 pandemic.

Further information regarding these programs and services can be found at:

https://www.westernsydney.edu.au/covid-itds

Further information about ITDS Protocols during the COVID-19 Pandemic can also be found:

Information Technology and Digital Services Protocols During the COVID-19 Pandemic

This document is specifically for people who have been provided a pre-configured computer as part of the COVID-19 Laptop program.

Need Additional Help?

If you need help, you can always call the IT Service Desk or search our online resources at:

https://www.westernsydney.edu.au/information_technology_services/its/servicedesk

COVID-19 Laptop Program

Purpose

These guidelines will provide basic information about the use of laptops issued under the COVID-19 laptop program, pre-installed with core software to assist front-line staff as they undertake their WSU duties from home.

About the COVID-19 Laptop Program

The COVID-19 Laptop Program is a crisis response initiative to assist with the unprecedented and urgent requirement that WSU staff undertake their duties in a work-from-home context. Appropriate WSU Management have nominated staff to receive laptops under the program. Information about the protocols underpinning the COVID-19 Laptop program, as well as other general tips and information relating to technology in a work from home context, are available on the ITDS Covid-19 page.

Unboxing your laptop

Inside the box of your temporary work from home (WFH) laptop, you will find:

- A DELL 5400 laptop;
- A Power Supply;
- A HDMI Cable; and
- Packaging and miscellaneous papers.

The laptops distributed under the COVID-19 Laptop Program are not standard University laptops. As such, you can expect that you may need to do some configuration and that operation may be slightly different than you would expect under ideal circumstances.

Expectations of recipients

Recipient of laptops under the COVID-19 Laptop Program are expected to:

- Take reasonable care of the laptop to minimise physical damage;
- Be hyper-vigilant about cyber security;
- Use the laptop only for University duties;
- Only install software required for University duties; and
- Return all equipment in the state that it was issued.

Returning your laptop

When you eventually return the laptop, you will need to return the entire contents of the box as received. Whilst you are using the laptop, please keep all the packaging and papers together in a safe place, ready for return to the University.

Damages and Peripherals

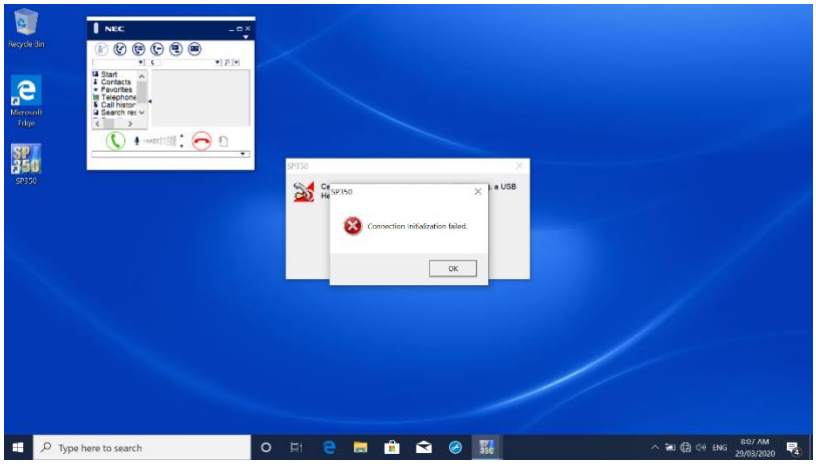
The document Information Technology and Digital Services Protocols During the COVID-19 Pandemic Provides further information on this

Getting Started: Powering up

1. Press the power button on the laptop (small round button near the delete key).
2. When presented with a screen image, press any key to take you to the login page.

- **Login Credentials:**
- **Username:** WSU_User (this will be pre-populated)
- **Password:** University1

3. When you press enter (or click the arrow to the right of the password box), you will be taken to the Windows Desktop.



- **PLEASE NOTE:** Don't worry if you see connection error messages at this stage. (as shown in the image above). You can click 'OK' to them.

4. For non-Windows users, the Windows icon in the lower left corner is the shortcut to all applications on the laptop. There are also some shortcuts along the bottom 'task bar' of the desktop.

5. Before you can do much, you will need to establish an internet connection (see the steps below)

Note: You may see messages asking you to undertake "DELL Updates" or similar. Running these updates is not required (press cancel or no if asked)

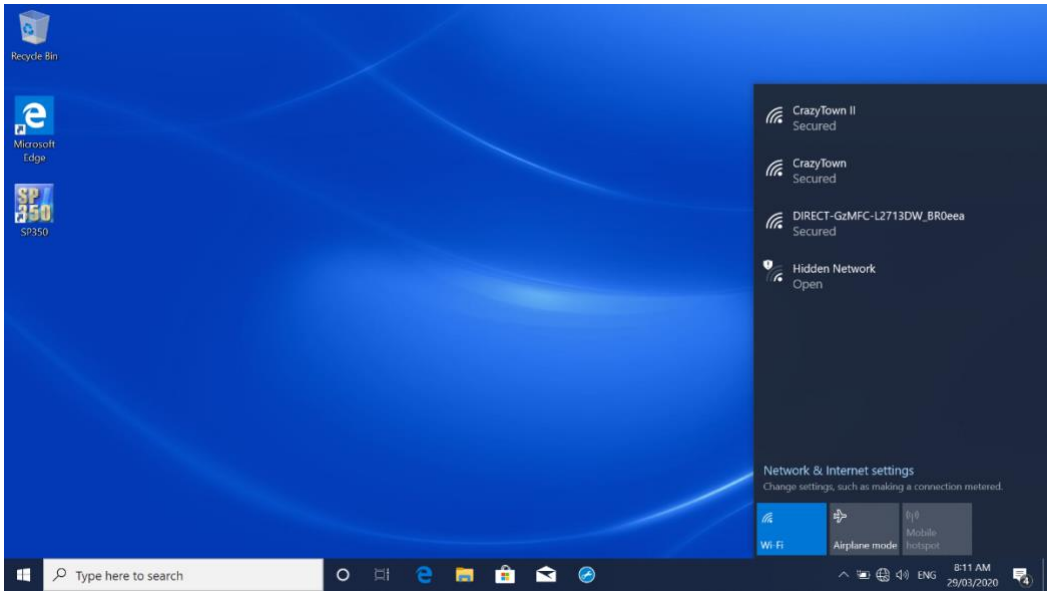
Getting Internet Access

Connect to your home wi-fi

The most reliable and the fastest method of connecting to the internet from home will be to connect to your pre-existing wi-fi network (if you have one).

To connect to your home wi-fi network you will need to know the "Access Key" (sometimes called the password) used for your wi-fi network.

1. From the Windows Desktop, click the small "Globe icon" in the bottom right of the taskbar. You will see a list of the available wi-fi networks (see image below).



   - **PLEASE NOTE:** that the wi-fi networks you see at home will be completely different to the ones shown in the pic above

2. Select your home wi-fi network, and enter the password. If you enter the password correctly, this should connect you to the internet through your home wi-fi network

Connect to your mobile phone 'hotspot'

If you do not have a home wi-fi network you may be able to use your mobile phone. When using this method, you need to be aware that you will be consuming your data-allowance provided by your mobile phone provider. If you exceed your data-allowance, you may incur charges from your mobile phone provider. These charges are not covered by the University. Please refer to your phone provider for any concessions available during the pandemic.

Accessing the University network

To access some University software (including QMaster, share drives, specialist equipment and SoftPhone), you will need access to the University network. You can get access to the University network by creating a Virtual Private Network (VPN).

Western has implemented a limited capacity VPN service which provides secure access to the University network through PC or Mac using a software client.

The VPN service provides secure access to:

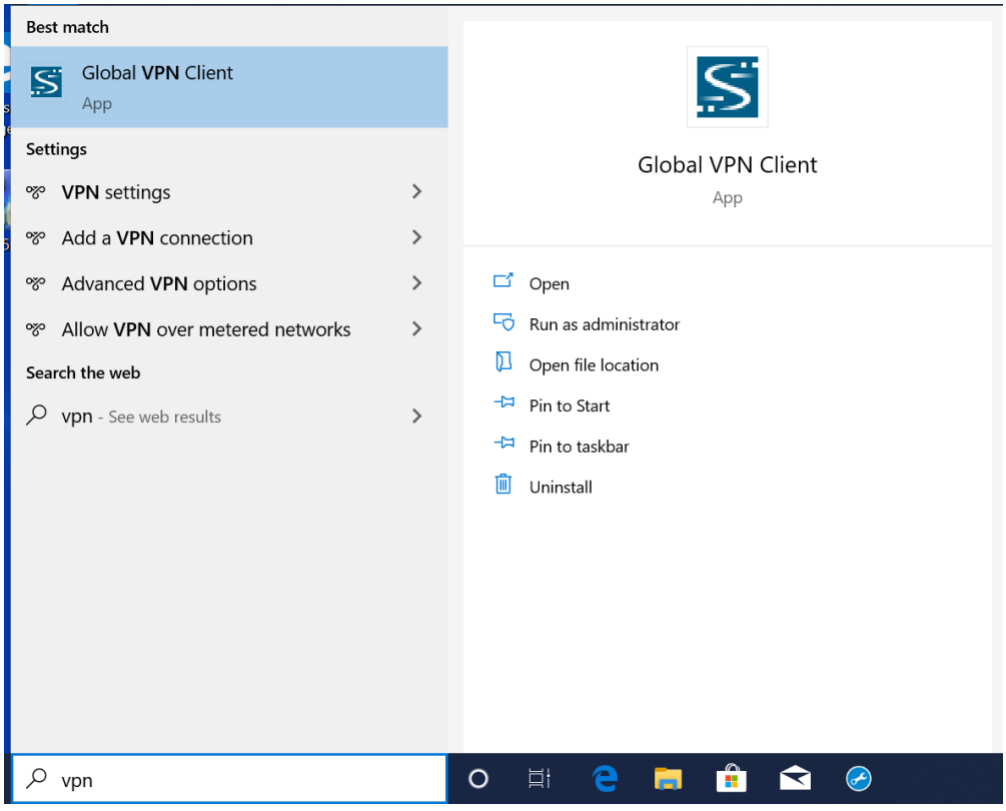
- Internally hosted services, only accessible via the Western network;
- Interactive services such as Secure Shell servers (SSH) and/or Remote Desktop Protocol (RDP) destinations;
- Specialist instrumentation connected directly to the Western network; and
- File shares e.g. My Documents.

Creating a Virtual Private Network (VPN)

Every time you wish to use software that requires a Western Network connection, you will need to create a Virtual Private Network (VPN). The VPN will be 'disabled' each time your laptop goes to sleep or turned off, meaning that you may need to re-establish your VPN.

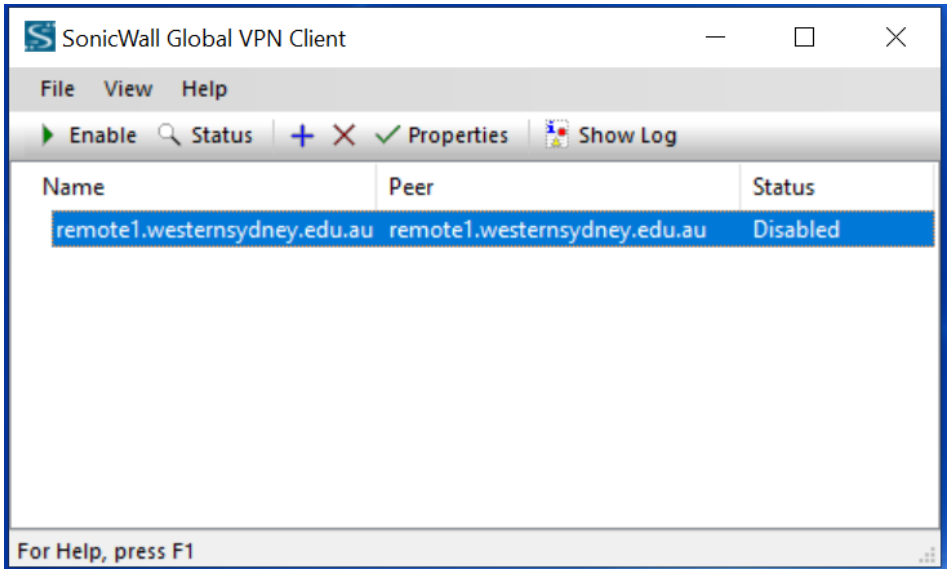
To create a VPN:

1. Click on the Windows icon in the lower left of the desktop and type "vpn". You should see 'Global VPN Client' appear.



2. Click "Global VPN Client"

3. Once the VPN client loads, you may/may not see a security warning, if you do, you need to accept. The VPN client will load and you will see a window as shown in the image below:



PLEASE NOTE:

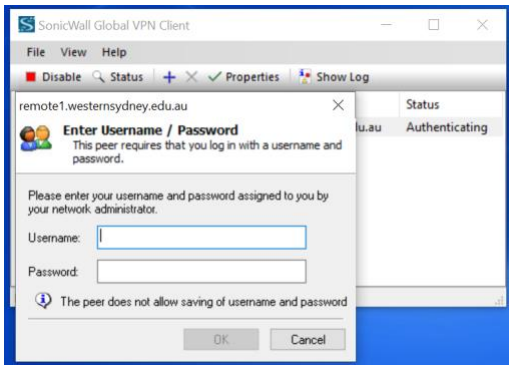
- the status of the VPN is 'Disabled' at this point; and
- The VPN has been pre-configured. You do not need to change/configure any settings.

4. Click "Enable"

5. The VPN will take some time to connect, depending on the internet connection you have. If you are using an internet connection through your mobile phone, it will take longer than through a home wi-fi network.
    a. As the VPN is connecting, note that the status has changed to "Connecting".

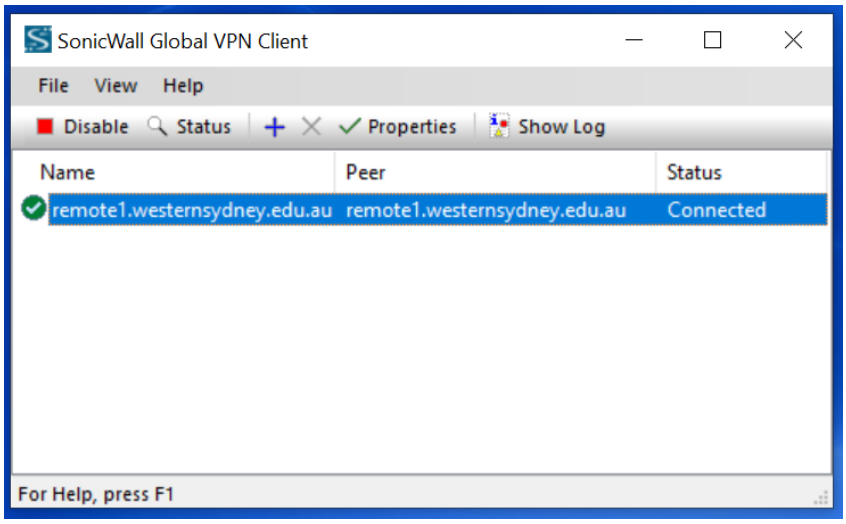
6. When the window appears asking for you username and password, please enter them. Your username is your staff ID and you password is your standard WSU password.

7. Click OK.

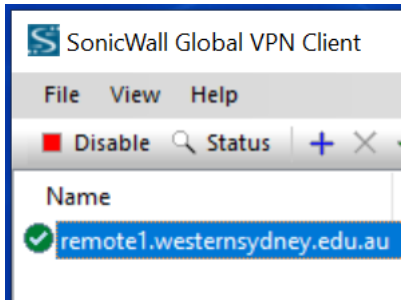


8. You may see a window warning you that "traffic is only allowed to this peer". This is OK. Click the check-box "If yes, don't show this dialog again" and then click 'yes'.

9. Assuming you have entered valid credentials, the VPN will then make the final connection and the status will change to "Connected". You will also get a notification at the bottom right of the windows desktop.



When finished doing your work that requires the University network, you should disable the VPN by clicking "Disable". Alternatively, closing the laptop will put it to sleep and disconnect the VPN.



Accessing Telephony Services Remotely

Using your Desk Phone remotely (NEC Softphone)

The laptop has been pre-installed with NEC Softphone software.

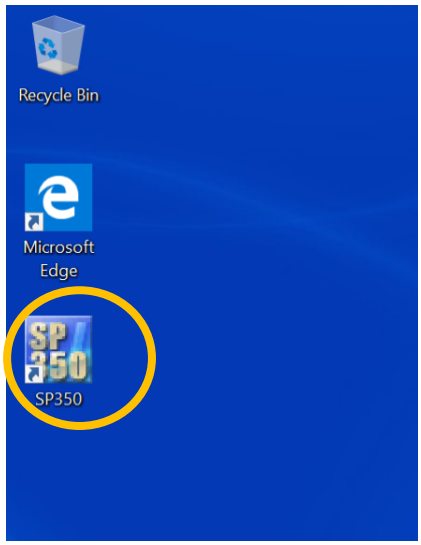
This software enables you to make and receive calls using your WSU desk phone number. Instead of a telephone handset, the software will use the inbuilt microphone and speakers of your computer. If you have a headset or earplugs, you can instead use these devices to make your phone calls.

PLEASE NOTE:

- You must be connected to the VPN to use NEC Softphone (Section 3); and
- You need to know your WSU desk phone extension number

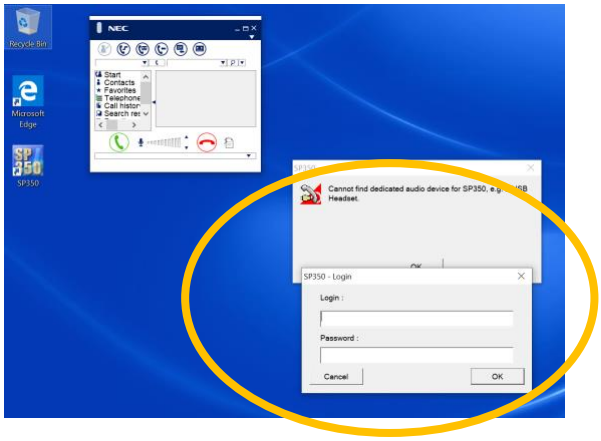
Using the NEC Softphone

1. Double click the SP350 icon on the desktop of your laptop

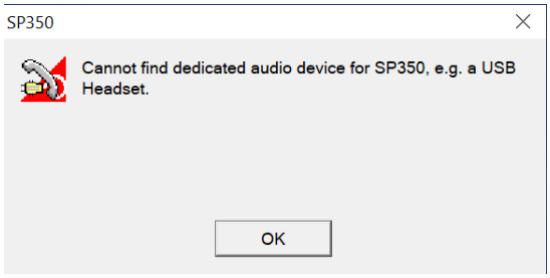


2. Enter login details

Login Details
Login: Your 4 digit desk phone extension Password: Your 4 digit desk phone extension



3. Click "OK" if you don't have a headset installed

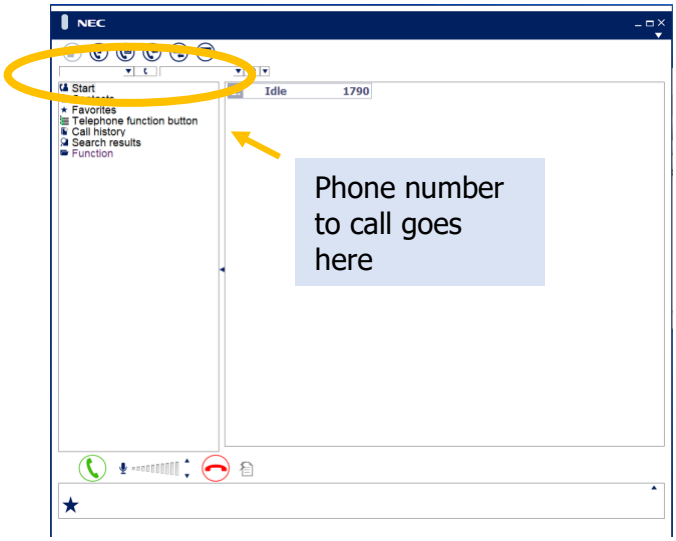


4. You should see the Softphone "Main Window"

5. The Main window has many features. There are many features available in this software. Only steps to make and answer a call are described below

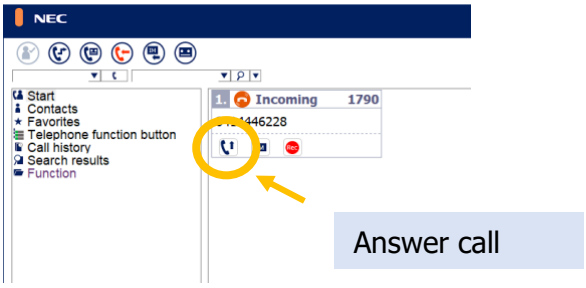
Make a Call

1. Insert the number to call in the box above the function list (shown below). You need to use a 'leading 0' before the number you wish to call. For example, if calling a mobile number, you would enter **0**0414 383 838
2. When the number has been entered, press the enter key on your keyboard to dial the number.
3. You can hang up using the red phone icon on the screen

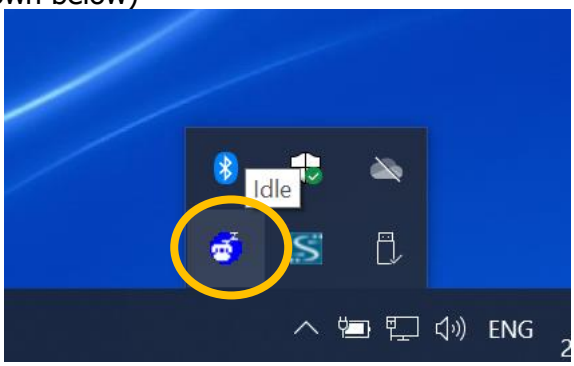


To Receive a call:

1. When you receive a call on your desk phone number, you will hear a phone ringing sound from your computer.
2. The softphone will show an incoming call and the number that is calling. You can answer the call using the small phone icon on the incoming call notification or using the 'green phone icon'



PLEASE NOTE: If your softphone disappears off the windows desktop (e.g. it gets minimised), you can re-open it by selecting the softphone icon from the task bar (as shown below)



University Call Centres & QMaster

The University will continue to operate its call centres on campus as long as it can and in the event of a closure, remotely where possible. The call centres are:

- Contact Service Centre
- Student Central
- Transition Success
- Western Success
- Client Services
- Team Student Experience, Administration and Enquiries
- IT Service Desk
- Human Resources

Staff in these call centres are considered critical forward-facing staff and as such, special technology considerations will apply in terms of laptop distribution, telephony support, etc.

Connecting to the VPN & Configuring SP350

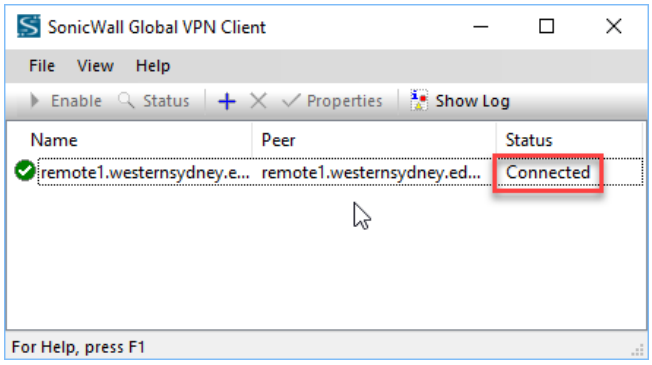
PLEASE NOTE: The following instructions are only for staff currently work in call centres, examples are listed above. Staff not working in these call centres, will not need to access to QMaster.

1. Restart the laptop.

2. On your desktop, please pen the application named **Connection to remote1.**

3. A new window will appear. Please enter your University **Staff ID** and **Password**, and select **OK**

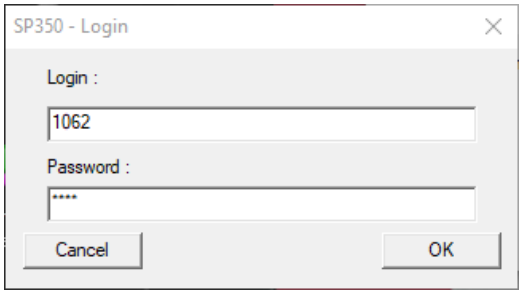
4. The window will close, and a new window will open showing your active connections. Leave the computer alone until the '**Status'** is '**Connected'** on the new window, as shown below.



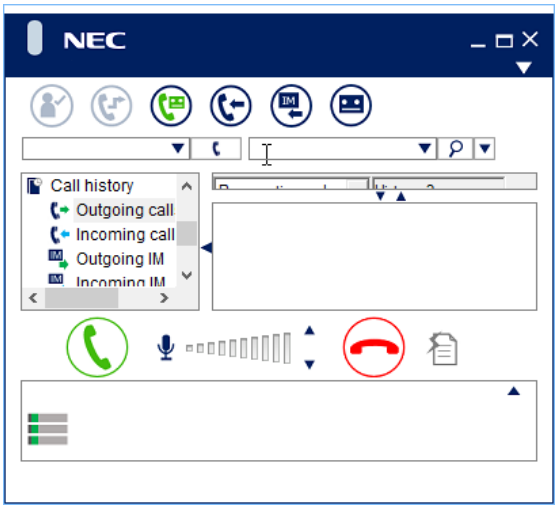
5. Open the Application Named **SP350** on your desktop

6. On the new window, enter the extension (4 digit number) of your desk phone in both the **username** and **password** field.

   *Note: If a new window appears advising the extension is already in use, select **yes***

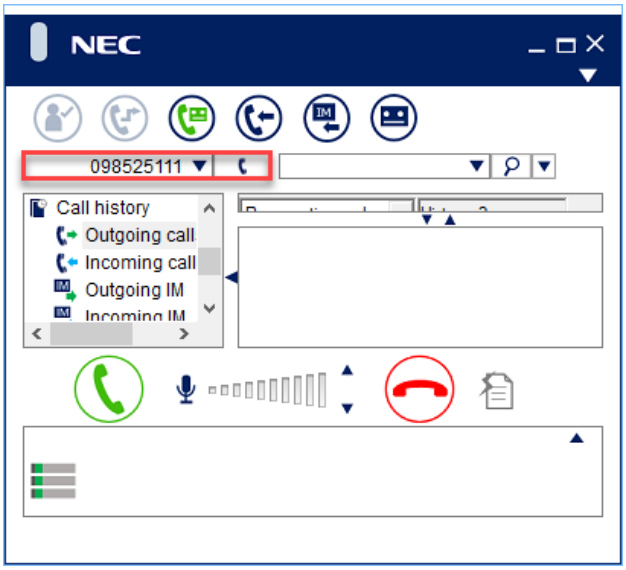


7. An NEC branded window will open. This is the application used to make & receive calls (Soft Phone). It should look like below:



8. To make a call, enter the number in the top left text box, and select the small phone icon.

   PLEASE NOTE: Extensions can be dialled as normal, but external numbers need correct prefixes like calling from a normal desk phone. (0 in front of a mobile for example)



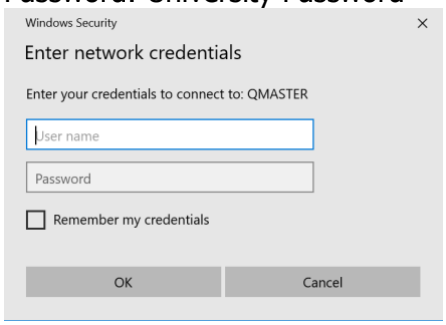
Connecting & Logging into QMaster

PLEASE NOTE: Opening and using QMaster will be slow when accessing it from home. Please allow AT LEAST a minute for functions such as logging in, and loading queues to process.

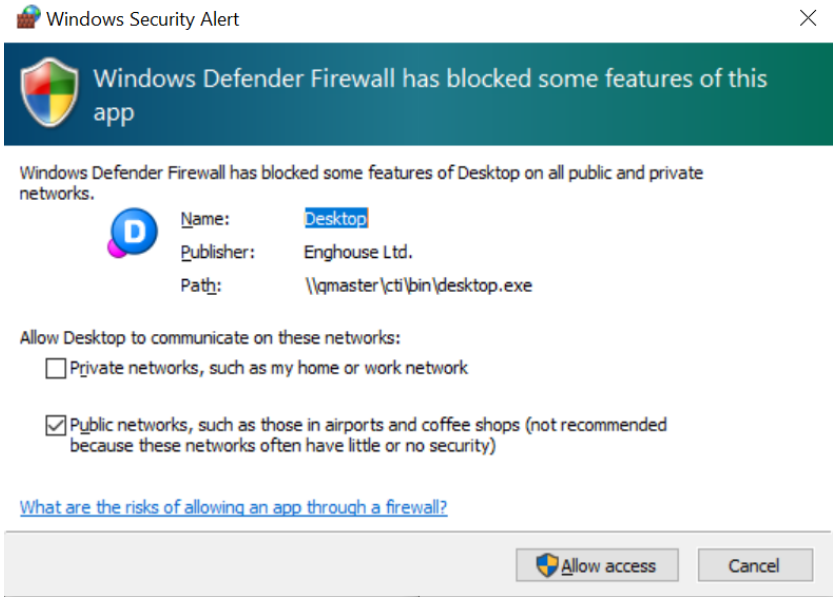
1. Once loaded, open the application Named **QMaster Desktop** on your desktop. **PLEASE NOTE:** This will take some time to open and initialise**.**

2. The first time you open this application, it will ask you to login. Please enter your Western Sydney credentials in the following format:

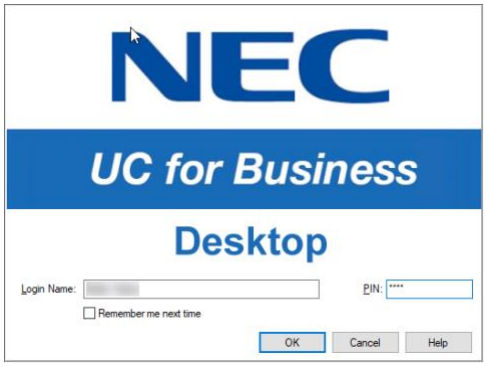
   Username: uws\staffID
   Password: University Password



3. Select the **Allow Access** button on the next Window:

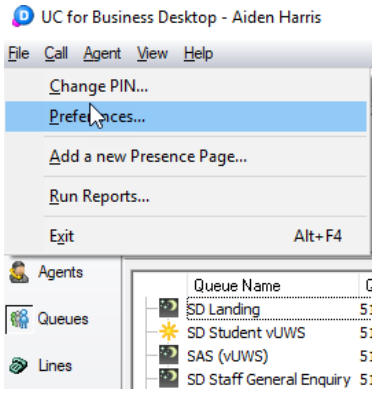


4. Login using your normal QMaster Credentials (Name & Pin)



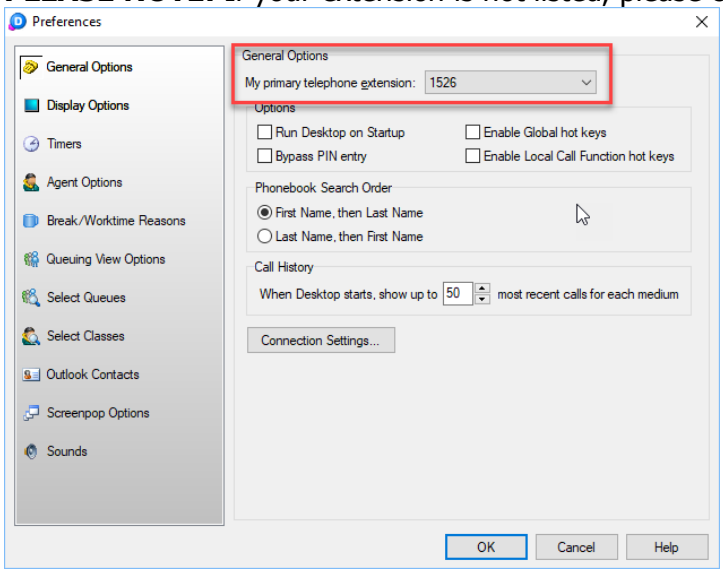
PLEASE NOTE: You MUST log out of QMaster on your desktop on campus before logging in remotely. If you do not log out, you will receive an error that you are already logged in, and QMaster will close.

5. Once opened, you need to make sure your extension is the same as what was entered on the **SP350** program. Select **File** > **Preferences** from the drop down.

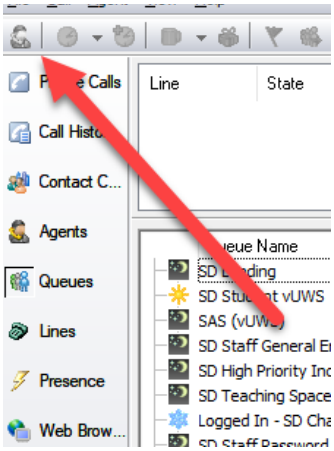


6. Under general options, select **the same extension you logged into SP350 with**, by selecting from the drop down list.

PLEASE NOTE: If your extension is not listed, please contact the IT Service Desk.



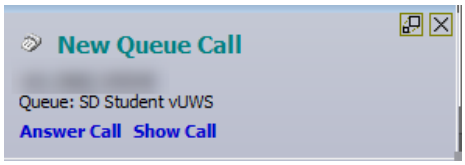
7. Select **OK**, and login to your normal login class using the person icon on the top left of the page.



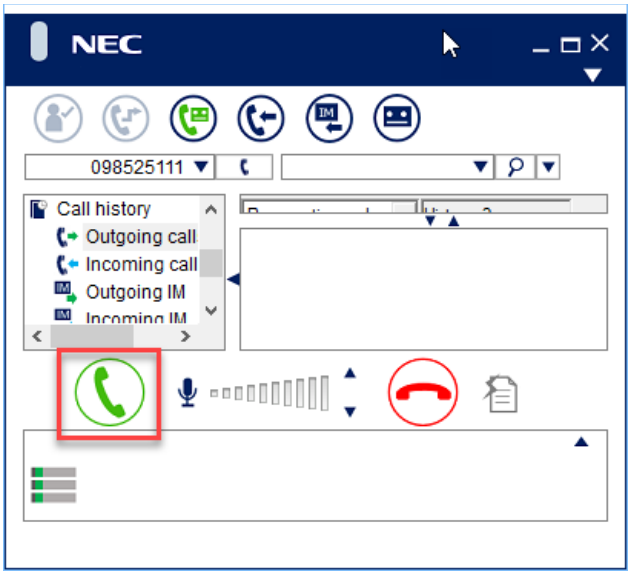
8. You should now be logged into relevant QMaster queues

Answering a Call

1. When receiving a queue call, you will receive a notification on your desktop (like usual). If you select **Answer Call**, it will answer the call through the Soft Phone.

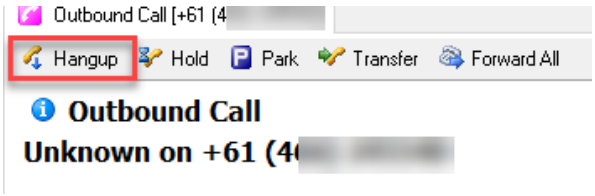


2. You can also select the **'Green Pickup'** button from the SP350 application to answer an incoming call:

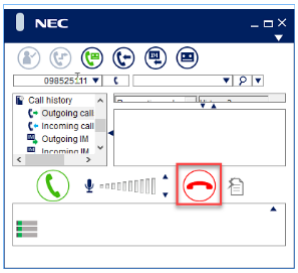


Ending a Call

1. To end a call, you can select the **Hang-up** option in QMaster:



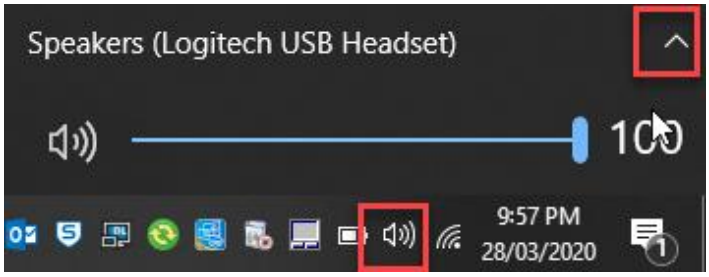
2. You can also select the '**Red Hang-up**' button from the SP350 application to end an existing call:



Configuring an External Audio Device for SP350 (Headphones and Microphones)

SP350 will use the default playback device on your computer. To use an external audio device, plugin the device **before** opening SP350.

1. Once your device is plugged in, select the audio icon on the right hand side of your task bar, screen, and select the ^ arrow on the right hand side of the menu.



2. This will list all connected audio devices. Select the desired audio device from the list, and close the menu.

Citrix

Citrix enables you to run University applications without having to install them on your device. To use Citrix all you need is a connection to the Internet. You do not need to connect to the University network using the VPN solution outlined previously.

To access Citrix, simply point your web browser to:

https://access.westernsydney.edu.au/logon/LogonPoint/index.html

Mac & tablet (iPad & Android) users that have compatibility problems accessing network folders, Staff eForms, Basware, Staff Online, MS Office and other applications, can use Citrix for a reliable, supported, and compatible experience.

In-depth instructions about how to use Citrix are contained in the knowledge base article: KB0014262.

Microsoft Office (Word, PowerPoint, Outlook, etc)

Using Microsoft Office suite of software (e.g. Microsoft Word, Excel, PowerPoint, OneNote etc.), has never been so easy. You have two choices:

- You can use the online version (browser based); or
- You can install the software onto the laptop.

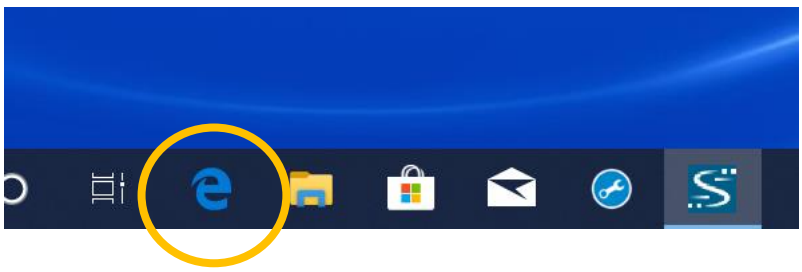
Installing on the Laptop

This will give you greater functionality where the performance will be much more reliable.

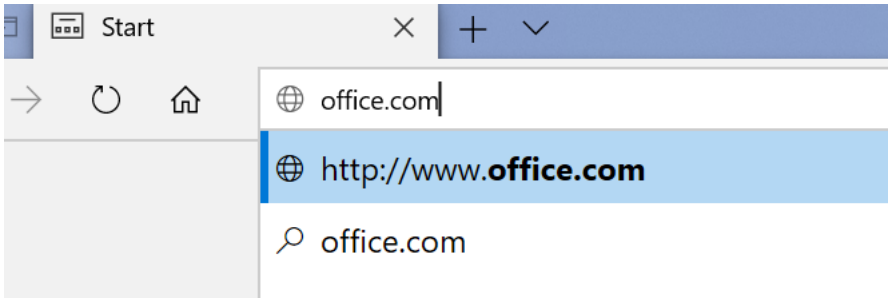
PLEASE NOTE: It is recommended that you install Microsoft Office using your home wi-fi internet access. Whilst possible, it is not recommended that you install Microsoft Office if accessing the internet through your mobile phone. The installation will consume a significant quantity of your data allowance and will be slow. If you don't have a home wi-fi internet access, you could use Microsoft Office online. Just visit www.office.com and 'sign in'.

Once connected to your home wi-fi internet connection, to install and use Microsoft Office on your laptop follow these steps:

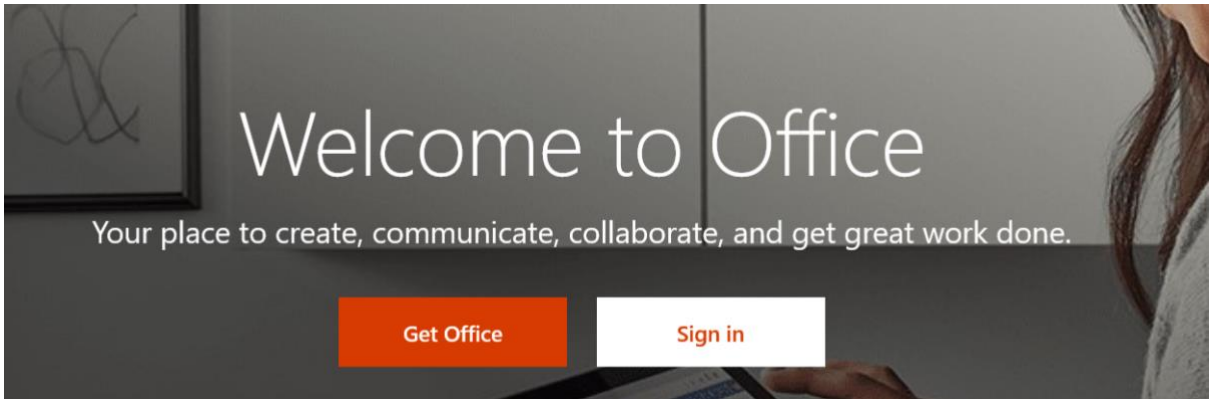
1. Open an internet browser (Microsoft Edge is pre-installed on the laptop).



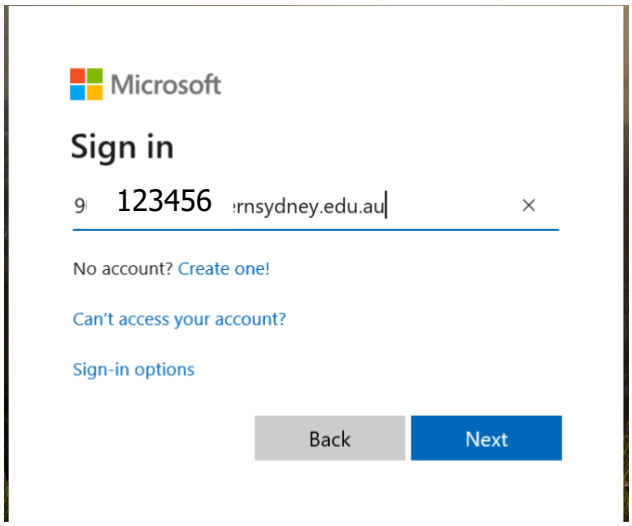
2. Navigate to www.officecom



3. Click "Sign In"



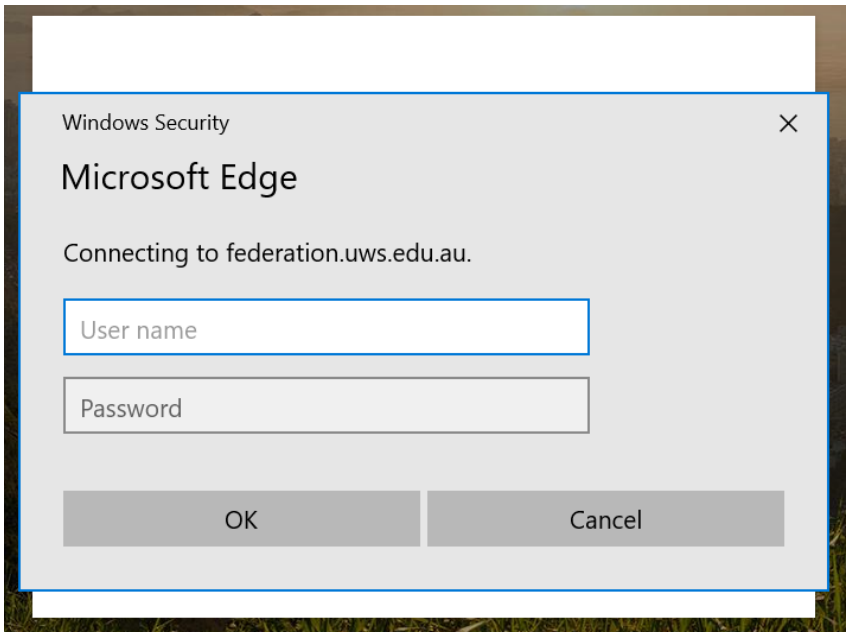
4. You Microsoft Login is your staff ID Number, followed by "@westersydney.edu.au"



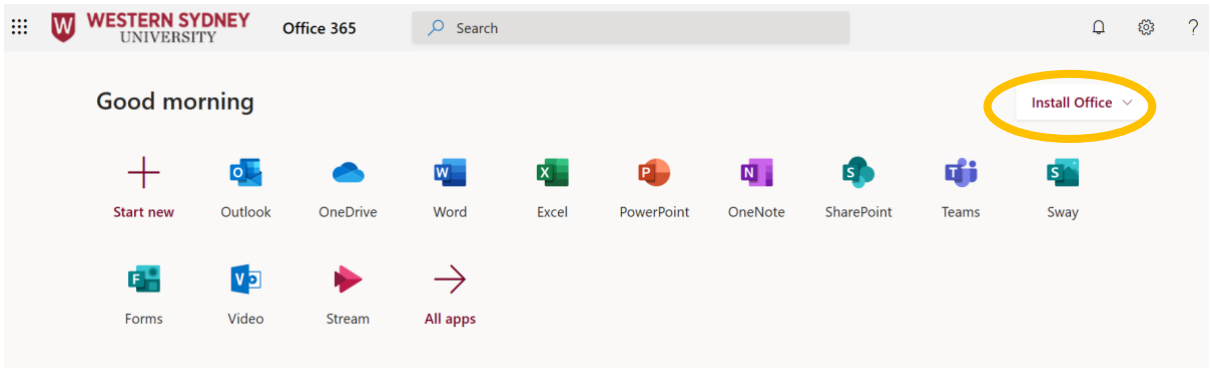
5. You may be asked to authenticate and enter your username again. This time the details are:

Login Details: **Username:** Your staff number (nothing more)

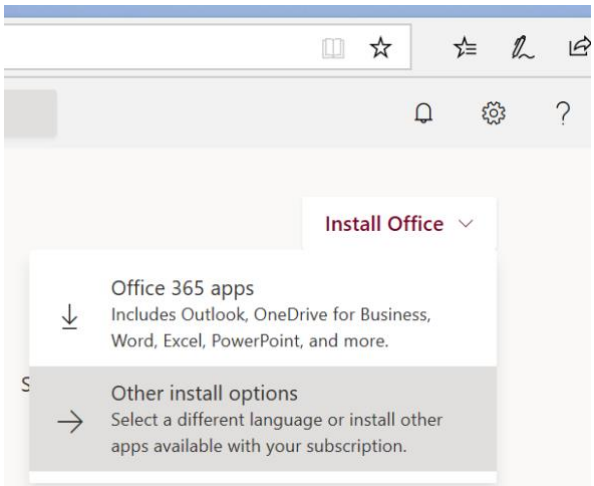
Password: usual WSU Staff Number



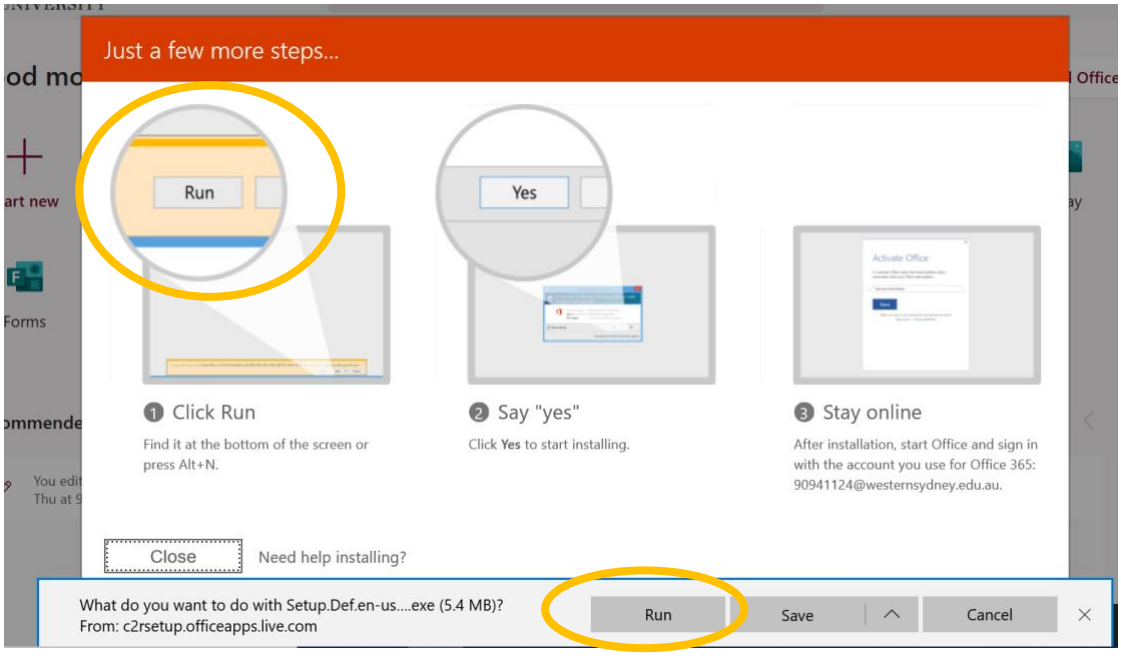
6. With the correct username and password, you will be taken into Office Online. Select "Install Office" in the top right of the window.



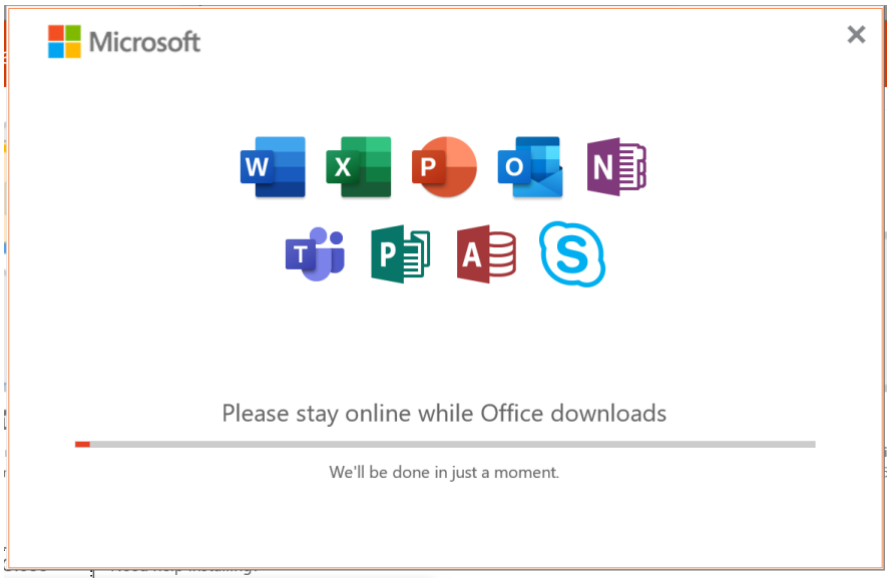
7. Select "Office 365 Apps"



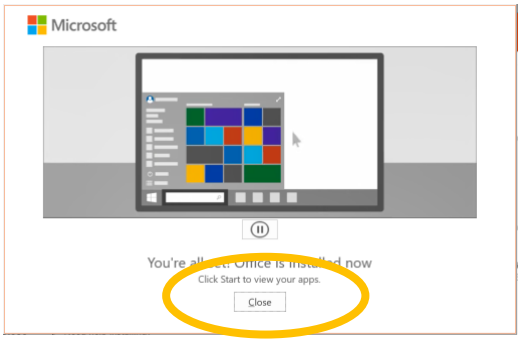
8. Click "Run"



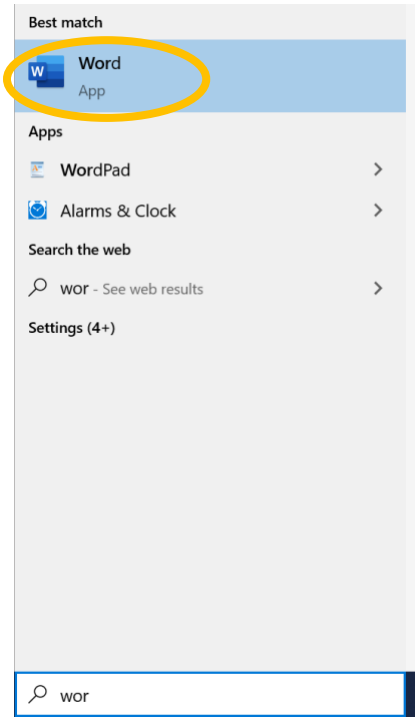
9. The Microsoft Office installer will start. The installation will take some time, depending on the speed of your internet connection. Just leave the installation to run



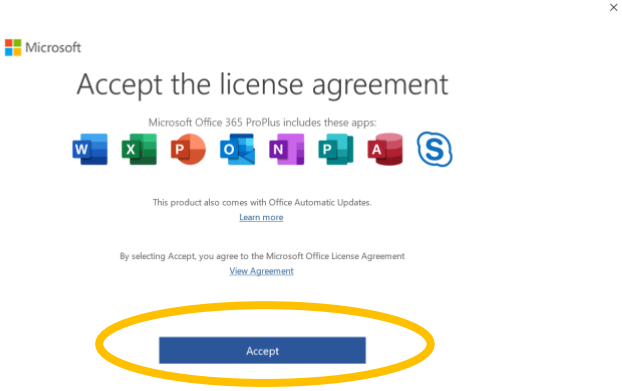
10. Once the installation is complete, you will see a confirmation message. Click "Close"



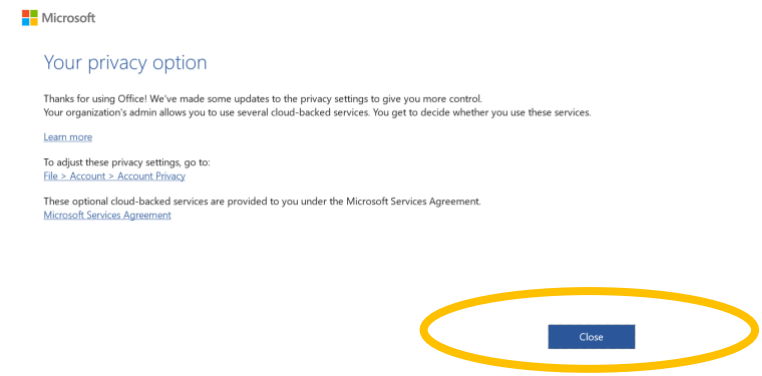
11. You should now be able to run any of the Microsoft applications. Click the windows icon at the bottom left of the screen and type "Word" (or Excel, PowerPoint, etc) and the icon for Microsoft Word should appear.



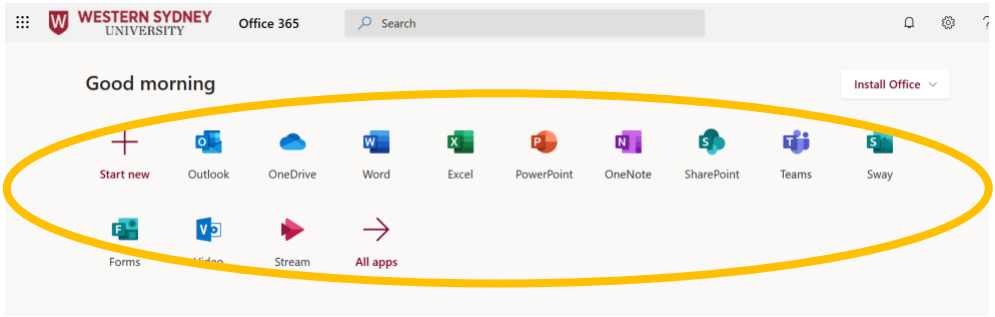
12. Accept the license agreement



13. Acknowledge the Privacy Information, and click "close"



That's it! You should be up and running with the Microsoft suite of products Remember, you can always use Microsoft Office online if you get stuck. Go to www.office.com and sign-in. Click any of the icons to use the online version of that product.



Other software not Pre-installed

If you need access to software that is not pre-installed on your temporary laptop, the ITDS Service Desk may be able to assist.

If requesting additional software, you should consider that your temporary laptop has not been set up with the 'Standard WSU Operating Environment'. As such, it may not be possible to install all software that would ordinarily be available on a WSU standard issue laptop or desktop.

Security: Safe & Secure Practices for Working from Home

Along with your health and well-being, it is equally important to ensure that you are individually secure and the University remains free from compromises. It is crucial that we work together during this time to protect our information. Here's some information and resources that ITDS have developed specifically to assist University staff in protecting themselves, their friends and family, and as a result the University at large

As we know, scammers are opportunistic and will use the COVID-19 pandemic to take advantage of staff and students. The simple rules are, make sure you:

- Run virus/malware protection software on any computer you use to do university work (all University-issued devices have this by default);
- Be extra vigilant for email phishing; and
- Report anything suspicious via the IT Service Desk.

Here some more tips from our **ITDS Security Corner** to help you when working from home:

Is your Antivirus Software Up-to-Date?	**Learn More**
University laptops come with antivirus installed, but If you're using a University laptop away from campus for an extended period of time, make sure that the antivirus is up-to-date. This will be the same for personal laptops, particularly as you will be using University systems and applications. It is important that you are protected. There are several trusted vendors such as: Sophos, McAfee, Norton, Bitdefender, Avast, Avira and Kaspersky. Still don't know which software to choose? The University currently uses Sophos for securing out desktops and laptops, and we have an arrangement offered through Sophos to provide the software to University employees for free. Please see the link provided.	Sophos Commercial Home version - (University email required)
Keep your Software up-to-date!	
It is equally important to keep your operating system and applications up-to-date, it will protect you being hacked. Try to make it a priority. By updating your devices, you will ensure that you do not have any vulnerabilities (weaknesses in software) so hackers, malicious programs or viruses will not exploit your computer or devices.	Software Updates | StaySmartOnline

Storing your Devices!	**Learn More:**
Make sure your devices are locked (or otherwise not accessible) when not in use – even if the device is a home computer, you are accessing University systems. Whether working on campus or from home, it is our collective responsibility to ensure personal and sensitive data held by the University isn't breached.	Storing your Devices | StaySmartOnline
Backup your Device Regularly	**Learn More:**
It is best practice is to make backups regularly. For University devices such as laptops, backups happen automatically whenever you're on campus. But, if you're going to be spending some extended time away from Campus, please note that this will not continue to happen. For personal devices, backups should be stored separately to the device itself, so that they can be accessed and used if the device is damaged, lost, or compromised.	World Backup Day Backups | StaySmartOnline
Don't Take the Bait! Phishing Scams	**Learn More:**
Phishing is a scam to try and steal your identity, your money, or both. Don't get hooked! Protect yourself and others: Be smart, be sceptical, be secure. • Avoid clicking on promotional links in emails • If there is general information that can be 'googled' and found, do that instead of clicking on a link from a suspicious sender • Don't click on baits such as an '80% discount on an exclusive cure' or 'treatment for coronavirus' • If unsure about the authenticity of a website, do not proceed with any login procedure	Email Security | Don't Take the Bait How to report Phishing and Spam email to ITDS
Sensitive Information	**Learn More:**
Take extra care to ensure the security of sensitive data when handling it away from campuses. University staff have responsibilities – including legal responsibilities – when it comes to handling data that is proprietary, sensitive, personal, or related to healthcare. If possible, place University data and documents you use for work in University storage (OneDrive, SharePoint, etc) so that you can avoid saving any copies of personal or sensitive data to a personal device. If you're not connected to the internet or this is otherwise	Confidential and Sensitive Information Considerations for Staff Personal Information and Privacy | StaySmartOnline Saving Docs to a SharePoint Portal

impossible, ensure any University data is removed from any personal device(s) used in the interim once you're back on campus. This also applies to any backups made during this time.	Microsoft Office | Saving Documents to OneDrive in Windows 10
WSU Cyber Security Learning Module	**Learn More:**
A Cyber Security overview training module has been procured by ITDS for all University staff. The module is called **'Cyber Security at Western Sydney University (Basics)'** and is accessible to University staff through MyCareerOnline and vUWS. Searching for 'cyber security' in MyCareerOnline will produce the module. Staff without access to MyCareerOnline, can enrol themselves in the vUWS site.	How-to-Access (PDF) Or visit ITDS' Security Corner website.

You can find more resources on the WSU website and WesternNow respectively, such as:

https://www.westernsydney.edu.au/covid-itds

Working Remotely – Help for Staff.